UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,364	07/17/2003	Colin John Blamires	03.028.01	8923

7590   09/01/2010

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER
SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
09/01/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

_____

Ex parte COLIN JOHN BLAMIRES, SIMON NEIL REED, and
MALCOLM DAVID BINNS

_____

Appeal 2009-005712
Application 10/620,364
Technology Center 2400

_____

Before ROBERT E. NAPPI, MAHSHID D. SAADAT,
and KARL D. EASTHOM, *Administrative Patent Judges*.

SAADAT, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

_____

[1] The two-month time period for filing an appeal or commencing a civil
action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing,
as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE"
(paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery
mode) shown on the PTOL-90A cover letter attached to this decision.

Appellant appeals under 35 U.S.C. § 134(a) from the Final Rejection
of claims 1-3, 7-11, 15-19, and 23-31. Claims 4-6, 12-14, and 20-22 have
been canceled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

STATEMENT OF THE CASE

The invention

Appellants' invention relates to detecting malware by providing a
bootable removable media that enables a clean boot to a non-installed
operating system to be performed (Spec. 2:4-6 and 3: 29-32). Claim 1 is
illustrative and reads as follows:

> 1.   A removable physical media bearing a computer program
> operable to control a computer to detect malware by performing the
> steps of:
>   booting said computer with a non-installed operating system
> read from said removable physical media instead of an installed
> operating system stored on said computer;
>   loading network support code for said computer read from said
> removable physical media;
>   downloading from a remote computer one or more malware
> detection files;
>   performing malware detection upon said computer using said
> one or more malware detection files; and
>   establishing a secure network connection to said remote
> computer;
>   wherein a firewall computer disposed between said computer
> and said remote computer is operable to block a connection between
> said computer and said remote computer other than said secure
> network connection;
>   wherein said network support code is used to enable said
> computer to establish said secure network connection via said firewall
> computer to said remote computer.

The applied prior art and rejections

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Reinert	US 6,347,375 B1	Feb. 12, 2002
McCoskey	US 2003/0028889 A1	Feb. 6, 2003
Yadav	US 2003/0149887 A1	Aug. 7, 2003
		(filed Feb. 1, 2002)
Khatri	US 6,721,883 B1	Apr. 13, 2004
		(filed Jan. 25, 2000)

Stallings, William, *Network Security Essentials, Applications and Standards*, 1999 Prentice-Hall, Inc., pp. 320-323 (hereinafter Stallings).

The rejections as presented by the Examiner are as follows:

Claims 1-3, 7-11, 15-19, 23-25, and 28-30 stand rejected as obvious under 35 U.S.C. § 103(a) over Reinert, Yadav, and Stallings.

Claims 26 and 27 stand rejected as obvious under 35 U.S.C. § 103(a) over Reinert, Yadav, and Stallings in view of Khatri.

Claim 31 stands rejected as obvious under 35 U.S.C. § 103(a) over Reinert, Yadav, and Stallings in view of McCoskey.[2]

We make reference to the Appeal Brief (filed Dec. 13, 2007), the Reply Brief (filed Apr. 10, 2008), and the Answer (mailed Mar. 5, 2008) for the respective positions of Appellants and the Examiner. Only those arguments actually made by Appellants have been considered in this decision. Arguments which Appellants did not make in the Briefs have not been considered and are deemed waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

---

[2] We do not consider Appellants' response to a rejection under 35 U.S.C. § 112 because no such rejection was included in the final rejection, nor was repeated in the Examiner's Answer.

Arguments

In rejecting claims 1-3, 7-11, 15-19, 23-25, and 28-30, the Examiner reads all the claimed elements on Reinert except for the claimed step of establishing a secure network connection to the remote computer for which the Examiner relies on Yadav and Stallings (Ans. 3-5). Appellants contend that combining the teachings of Yadav where currently running network applications are taken into consideration cannot be combined with Reinert which is concerned with situations where the normal operating system of the local computer is not operable (App. Br. 11-12). Appellants further assert that the specific portions of the references relied on by the Examiner do not teach that "network support code is used to <u>enable</u> said computer to establish said secure network connection <u>via said firewall</u> computer to said remote computer," as recited in claim 1 (App. Br. 12-13).

With respect to claims 29 and 30, Appellants contend (App. Br. 13-15) that Reinert's downloading a program from the remote computer is not the same as determining the malware detection files based on the non-installed operating system and a malware detection product, respectively.

Regarding the rejection of claims 26, 27, and 31, Appellants rely on the same arguments made for claim 1 (App. Br. 15-16).

ISSUES

Appellants' arguments present the following issues:

1.   Has the Examiner erred in rejecting claim 1 by finding that the combination of the Reinert with Yadav and Stallings teaches the claim feature of "said network support code is used to enable said computer to

establish said secure network connection via said firewall computer to said remote computer?"

    2.   Has the Examiner erred in rejecting claims 29 and 30 by finding that Reinert teaches determining the malware detection files based on the non-installed operating system or a malware detection product?

FINDINGS OF FACT

The following findings of fact (FF) are relevant to the issues involved in the appeal.

    1.   Reinert discloses a method and apparatus for providing up-to-date virus scanning of a local computer by a remote computer comprising those situations where the normal operating system of the local computer is not operable. (Col. 3, ll. 41-48.)

    2.   As shown in Figure 2, Reinert discloses "that the local computer 42 may boot up even if its normal operating system program has been rendered inoperable by a virus or other catastrophic event." (Col. 7, ll. 48-50.) A bootable virus utility operating program comprising virus utility and communications software programs is loaded into the local computer memory 41. The virus utility and communications software programs are contained in a removable storage medium, e.g. floppy diskette, ZIP drive, CD-ROM etc., or in a fixed storage medium such as a separately allocated boot sector of a hard disk data storage device 44. (Col. 7, ll. 47-59.)

    3.   After the local computer 42 boots up, the user may choose to execute a virus scanning program and if one or more viruses are detected on the local computer 42, the user may connect to the remote computer 54. In that case, a communications program is invoked by the local user to

establish a communications connection between the local computer 42 and the remote computer 54 via the communications hardware modems 40 and 58, respectively. (Col. 7, l. 60 – col. 8, l. 3.)

     4.   Once communications is established and the remote computer 54 takes over control of the local computer 42, the local user may then conduct data recovery, virus scanning, or virus repair operations, under the control of the remote computer 54 by selecting a service, wherein a service program is downloaded from the remote computer 54 to the local computer 42, via communications hardware modem 58 and 40, respectively, and stored in the local computer memory 41. (Col. 8, ll. 10-19.)

     5.   If the local computer 42 requests virus scanning services, a virus scanning software utility program is downloaded into the local computer memory 41. In addition, a complete up-to-date virus signature file is downloaded into the local computer memory 41, which is advantageous in data recovery applications because the virus scanning and virus repairing programs may be executed in the local computer memory 41 without having to over-write any data located on the hard disk drive 44. The remote computer 54 maintains up-to-date the virus signature file containing the signatures of the latest known viruses. (Col. 8, ll. 20-39.)

PRINCIPLES OF LAW

     On the issue of obviousness, the Supreme Court has stated that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007).

> [A]n implicit motivation to combine exists . . . when the
> "improvement" is technology-independent and the combination of
> references results in a product or process that is more desirable, for
> example because it is stronger, cheaper, cleaner, faster, lighter,
> smaller, more durable, or more efficient. Because the desire to
> enhance commercial opportunities by improving a product or process
> is universal . . . there exists in these situations a motivation to combine
> prior art references even absent any hint of suggestion in the
> references themselves. In such situations, the proper question is
> whether the ordinary artisan possesses knowledge and skills rendering
> him *capable* of combining the prior art references.

DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co., 464
F.3d 1356, 1368 (Fed. Cir. 2006).

ANALYSIS

1.   Claim 1

Based on our review of Reinert, we agree with the Examiner's finding
(Ans. 17) that the disclosed local computer in Reinert may boot up even if a
virus or a catastrophic event has rendered the computer's operating system
program inoperable (FF2). In that regard, while Reinert provides up-to-date
virus scanning of a local computer by a remote computer when the normal
operating system of the local computer is not operable (FF 1), the term
"even if" indicates that the virus scanning takes place when the local
computer's operating system is operable as well as when it is inoperable.
Therefore, contrary to Appellants' arguments (Reply Br. 3), the condition of
virus scanning described in Reinert also applies to situations wherein the
normal operating system of the local computer is operable.

We further remain unconvinced by Appellants' argument (App. Br.
12-13) that the claimed "said network support code is used to <u>enable</u> said

computer to establish said secure network connection <u>via said firewall</u>
computer to said remote computer" (emphasis added) is not taught by the
applied prior art. As stated by the Examiner (Ans. 18), Reinert uses a
bootable media to boot the local computer and execute the virus scan (FF 2).
Specifically, we find that the local computer in Reinert may contact the
remote computer when a communications program is invoked by a local user
(FF 3), which meets the claimed "loading network support code."

We also agree with the Examiner (Ans. 18-19) that the
communications connection between the local computer and the remote
computer in Reinert would have benefited from the added security taught by
Yadav and the firewall of Stallings during the virus scan operation (FF 4).
Appellants' argument (Reply Br. 5-6) that including a firewall that allows
only authorized connections does not teach or suggest the claimed features
related to the network support code also not convincing. As the Examiner
found (Ans. 19), Reinert's system of invoking a communications program
by the user in combination with Yadav's firewall benefits from applying
some type of code to authorize the connection before the virus scanning
services start (*See* FF 4 and 5).

Therefore, we find that the Examiner did not err in rejecting claim 1
by combining Reinert, Yadav, and Stallings and finding that the combination
of Reinert with Yadav and Stallings teaches the claim feature of "said
network support code is used to enable said computer to establish said
secure network connection via said firewall computer to said remote
computer."

2.   *Claims 29 and 30*

Claim 29 requires that the malware detection filed are determined based on the non-installed operating system without specifying which entity makes the determination (*see* claim 29). Reinert discloses that the service selected by the user is downloaded from the remote computer to the local computer (FF 4), such as a virus scanning software utility program which is downloaded into the local computer memory (FF 5). Therefore, as asserted by the Examiner (Ans. 20), the malware detection files are determined based on the scanning program and the communications program invoked by the user (FF 4 and 5). In other words, the remote computer or the user downloads the malware detection software based on the non-installed operating system and the invoked communications program.

Similarly, claim 30 requires determining the malware detection files based on a malware detection product (*see* claim 30), which reads on determining downloaded files for virus scanning files by either the user or the remote computer in Reinert. *See* FF 4 and 5. For the same reasons stated above regarding claim 29, we agree with the Examiner (Ans. 20-21) that the downloaded malware detection files are based on the user invoked communications program and the specific virus scanning service requested (FF 5).

Thus, the Examiner did not err in rejecting claims 29 and 30 by finding that Reinert teaches determining the malware detection files based on the non-installed operating system or a malware detection product.

CONCLUSION

On the record before us and as discussed above, we find no error in the Examiner's position rejecting claims 1, 29, and 30. Accordingly, the 35 U.S.C. § 103(a) rejection of claims 1, 29, and 30, as well as claims 2, 3, 7-11, 15-19, 23-25, and 28 which are not argued separately, is sustained. We also sustain the 35 U.S.C. § 103(a) rejections of claims 26, 27, and 31 because Appellants provide no specific arguments for these claims and allow them to fall with claim 1 (App. Br. 21-22).

ORDER

The decision of the Examiner rejecting claims 1-3, 7-11, 15-19, and 23-31 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

gvw

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120